United Nations A/CN.9/WG.IV/WP.86

General Assembly

Distr.: Limited
18 August 2000

Original: English

United Nations Commission
on International Trade Law
Working Group
on Electronic Commerce
Thirty-seventh session
Vienna, 18-29 September 2000

Electronic Signatures

Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures

Note by the Secretariat

1. Pursuant to decisions taken by the Commission at its twenty-ninth (1996) [1] and thirtieth (1997) [2] sessions, the Working Group on Electronic Commerce devoted its thirty-first to thirty-sixth sessions to the preparation of the draft UNCITRAL Uniform Rules of Electronic Signatures (hereinafter referred to as "the Uniform Rules"). Reports of those sessions are found in documents A/CN.9/437, 446, 454, 457, 465 and 467. In preparing the Uniform Rules, the Working Group noted that it would be useful to provide in a commentary additional information concerning the Uniform Rules. Following the approach taken in the preparation of the UNCITRAL Model Law on Electronic Commerce, there was general support for a suggestion that the draft Uniform Rules should be accompanied by a guide to assist States in enacting and applying the Uniform Rules. The guide, much of which could be drawn from the *travaux préparatoires* of the Uniform Rules, would also be helpful to other users of the Uniform Rules.

2. At its thirty-sixth session, the Working Group discussed the issue of electronic signatures on the basis of the note prepared by the Secretariat (A/CN.9/WG.IV/WP.84). After discussion, the Working Group adopted the substance of draft articles 1 and 3 to 11 of the Uniform Rules and referred them to a drafting group to ensure consistency between the provisions of the Uniform Rules. The Secretariat was requested to prepare a draft guide to enactment of the provisions adopted. Subject to approval by the Commission, the Working Group recommended that draft articles 2 and 13 of the Uniform Rules, together with the guide to enactment, be reviewed by the Working Group at a future session. [3]

3. At its thirty-third session (June-July 2000), the Commission noted that the Working Group, at its thirty-sixth session, had adopted the text of draft articles 1 and 3 to 12 of the Uniform Rules. It was stated that some issues remained to be clarified as a result of the decision by the Working Group to delete the notion of enhanced electronic signature from the Uniform Rules. A concern was expressed that, depending on the

V.00-56533

decisions to be made by the Working Group with respect to draft articles 2 and 13, the remainder of the draft provisions might need to be revisited to avoid creating a situation where the standard set forth by the uniform rules would apply equally to electronic signatures that ensured a high level of security and to low-value certificates that might be used in the context of electronic communications that were not intended to carry significant legal effect.

4. After discussion, the Commission expressed its appreciation for the efforts extended by the Working Group and the progress achieved in the preparation of the Uniform Rules. The Working Group was urged to complete its work with respect to the Uniform Rules at its thirty-seventh session and to review the draft guide to enactment to be prepared by the Secretariat. [4]

5. The annex to the present note contains Part One and Chapter I of Part Two of the draft Guide prepared by the Secretariat. Chapter II of Part Two is published in document A/CN.9/WG.IV/WP.86/Add.1.

Annex

UNCITRAL
UNIFORM RULES ON
ELECTRONIC SIGNATURES

WITH

GUIDE TO ENACTMENT

2001

CONTENTS

General Assembly Resolution .....

Part One

UNCITRAL UNIFORM RULES ON ELECTRONIC SIGNATURES (2001)

Preamble

		Page
Article 1.	Sphere of application	6
Article 3.	Equal treatment of signature technologies	6
Article 4.	Interpretation	6
Article 5.	Variation by agreement	7
Article 6.	Compliance with a requirement for a signature	7
Article 7.	Satisfaction of article 6	7
Article 8.	Conduct of the signatory	8
Article 9.	Conduct of the supplier of certification services	8
Article 10.	Trustworthiness	9
Article 11.	Conduct of the relying party	9

Part Two

GUIDE TO ENACTMENT OF THE UNCITRAL UNIFORM RULES ON ELECTRONIC SIGNATURES (2001)

		Paragraphs	*Page*
Purpose of this Guide		1-2	11
Chapter I. Introduction to the Uniform Rules		3-84	11
I.	Purpose and origin of the Uniform Rules	3-24	11
A.	Purpose	3-5	11
B.	Background	6-11	12
C.	History	12-24	12
II.	The Uniform Rules as a tool for harmonizing laws	25-26	16
III.	General remarks on electronic signatures	27-61	16

		Paragraphs	Page
A.	Functions of signatures	27-28	16
B.	Digital signatures and other electronic signatures	29-61	17
1.	Electronic signatures relying on techniques other than public-key cryptography	31-33	17
2.	Digital signatures relying on public-key cryptography	34-61	18
(a)	Technical notions and terminology	35-43	18
(i)	Cryptography	35-36	18
(ii)	Public and private keys	37-38	19
(iii)	Hash function	39	19
(iv)	Digital signature	40-41	19
(v)	Verification of digital signature	42-43	20
(b)	Public key infrastructure (PKI) and suppliers of certification services	44-60	20
(i)	Public key infrastructure (PKI)	49-51	21
(ii)	Supplier of certification services	52-60	22
(c)	Summary of the digital signature process	61	24
IV	Main features of the Uniform Rules	62-81	25
A.	Legislative nature of the Uniform Rules	62-63	25
B.	Relationship with the UNCITRAL Model Law on Electronic Commerce	64-67	25
1.	Uniform Rules as a separate instrument	64	25
2.	Uniform Rules fully consistent with the Model Law	65-66	25
3.	Relationship with article 7 of the Model Law	67	26
C.	"Framework" rules to be supplemented by technical regulations and contract	68-69	26
D.	Added certainty as to the legal effects of electronic signatures	70-75	26
E.	Basic rules of conduct for the parties involved	76-80	28
F.	A technology-neutral framework	81	29
V.	Assistance from the UNCITRAL Secretariat	82-84	29
A.	Assistance in drafting legislation	82-83	29
B.	Information on the interpretation of legislation based on the Uniform Rules	84	29

Chapter II. Article-by-article remarks (see A/CN.9/WG.IV/WP.86/Add.1)

Title		1	3
Article 1.	Sphere of application	2-6	3
Article 3.	Equal treatment of signature technologies	7	5
Article 4.	Interpretation	8-10	6
Article 5.	Variation by agreement	11-14	7
Article 6.	Compliance with a requirement for a signature	15-28	8
Article 7.	Satisfaction of article 6	29-33	12
Article 8.	Conduct of the signatory	34-38	13
Article 9.	Conduct of the supplier of certification services	39-42	15
Article 10.	Trustworthiness	43	17
Article 11.	Conduct of the relying party	44-47	18

Part One

UNCITRAL UNIFORM RULES ON ELECTRONIC SIGNATURES (2001)

Draft articles 1 and 3 to 11 of the UNCITRAL Uniform Rules on Electronic Signatures (2001)

(as adopted by the UNCITRAL Working Group on Electronic Commerce at its thirty-sixth session, held in New York from 14 to 25 February 2000)

Article 1. Sphere of application

These Rules apply where electronic signatures are used in the context* of commercial** activities. They do not override any rule of law intended for the protection of consumers.

*The Commission suggests the following text for States that might wish to extend the applicability of these Rules:

"These Rules apply where electronic signatures are used, except in the following situations: [...]."

**The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 3. Equal treatment of signature technologies

None of these Rules, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 (1) of these Rules or otherwise meets the requirements of applicable law.

Article 4. Interpretation

(1) In the interpretation of these Rules, regard is to be had to their international origin and to the need to promote uniformity in their application and the observance of good faith.

(2) Questions concerning matters governed by these Rules which are not expressly settled in them are to be settled in conformity with the general principles on which these Rules are based.

Article 5. Variation by agreement

These Rules may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under the law of the enacting State [or unless otherwise provided for in these Rules].

Article 6. Compliance with a requirement for a signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

(a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;

(b) the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Paragraph (3) does not limit the ability of any person:

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

(5) The provisions of this article do not apply to the following: [...]

Article 7. Satisfaction of article 6

(1) *[Any person, organ or authority, whether public or private, specified by the enacting State as competent]* may determine which electronic signatures satisfy the provisions of article 6.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

(3) Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

(1) Each signatory shall:

(a) exercise reasonable care to avoid unauthorized use of its signature device;

(b) without undue delay, notify any person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) the signatory knows that the signature device has been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature device may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

(2) A signatory shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 9. Conduct of the supplier of certification services

(1) A supplier of certification services shall:

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

(i) the identity of the supplier of certification services;

(ii) that the person who is identified in the certificate had control of the signature device at the time of signing;

(iii) that the signature device was operational on or before the date when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) the method used to identify the signatory;

(ii) any limitation on the purpose or value for which the signature device or the certificate may be used;

(iii) that the signature device is operational and has not been

compromised;

(iv) any limitation on the scope or extent of liability stipulated by the supplier of certification services;

(v) whether means exist for the signatory to give notice that a signature device has been compromised;

(vi) whether a timely revocation service is offered;

(e) provide a means for a signatory to give notice that a signature device has been compromised, and ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

[Article 10. Trustworthiness

In determining whether and the extent to which any systems, procedures and human resources utilized by a supplier of certification services are trustworthy, regard shall be had to the following factors:

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the supplier of certification services regarding compliance with or existence of the foregoing; and

(g) any other relevant factor.]

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and

(ii) observe any limitation with respect to the certificate.

Part Two

GUIDE TO ENACTMENT OF THE UNCITRAL UNIFORM RULES ON ELECTRONIC SIGNATURES (2001)

Purpose of this Guide

1. In preparing and adopting the UNCITRAL Uniform Rules on Electronic Signatures (also referred to in this publication as "the Uniform Rules"), the United Nations Commission on International Trade Law (UNCITRAL) was mindful that the Uniform Rules would be a more effective tool for States modernizing their legislation if background and explanatory information were provided to executive branches of Governments and legislators to assist them in using the Uniform Rules. The Commission was also aware of the likelihood that the Uniform Rules would be used in a number of States with limited familiarity with the type of communication techniques considered in the Uniform Rules. This Guide, much of which is drawn from the *travaux préparatoires* of the Uniform Rules, is also intended to be helpful to other users of the text, such as judges, arbitrators, practitioners and academics. Such information might also assist States in considering which, if any, of the provisions should be varied in order to be adapted to any particular national circumstances necessitating such variation. In the preparation of the Uniform Rules, it was assumed that the draft Uniform Rules would be accompanied by such a guide. For example, it was decided in respect of a number of issues not to settle them in the Uniform Rules but to address them in the Guide so as to provide guidance to States enacting the Uniform Rules. The information presented in this Guide is intended to explain why the provisions in the Uniform Rules have been included as essential basic features of a statutory device designed to achieve the objectives of the Uniform Rules.

2. The present Guide to Enactment has been prepared by the Secretariat pursuant to the request of UNCITRAL made at the close of its thirty-fourth session, in 2001. It is based on the deliberations and decisions of the Commission at that session,[8] when the Uniform Rules were adopted, as well as on considerations of the Working Group on Electronic Commerce, which conducted the preparatory work.

Chapter I. Introduction to the Uniform Rules

I. PURPOSE AND ORIGIN OF THE UNIFORM RULES

A. Purpose

3. The increased use of electronic authentication techniques as substitutes for hand-written signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as "electronic signatures"). The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal (as well as technical) interoperability is essential.

4. Building on the fundamental principles underlying article 7 of the UNCITRAL Model Law on Electronic Commerce (also referred to in this publication as "the Model

Law") with respect to the fulfilment of the signature function in an electronic environment, the Uniform Rules are designed to assist States in establishing a modern, harmonized and fair legislative framework to address more effectively the issues of electronic signatures. In a modest but significant addition to the Model Law, the Uniform Rules offer practical standards against which the technical reliability of electronic signatures may be measured. In addition, the Uniform Rules provide a linkage between such technical reliability and the legal effectiveness that may be expected from a given electronic signature. The Uniform Rules add substantially to the Model Law by adopting an approach under which the legal effectiveness of a given electronic signature technique may be pre-determined (or assessed prior to being actually used). The Uniform Rules are thus intended to foster the understanding of electronic signatures, and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions. Moreover, by establishing with appropriate flexibility a set of basic rules of conduct for the various parties that may become involved in the use of electronic signatures (i.e., signatories, relying parties and third-party service providers) the Uniform Rules may assist in shaping more harmonious commercial practices in cyberspace.

5. The objectives of the Uniform Rules, which include enabling or facilitating the use of electronic signatures and providing equal treatment to users of paper-based documentation and users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Uniform Rules (and the Model Law) in its national legislation for those situations where parties opt to use electronic means of communication, an enacting State would appropriately create a media-neutral environment.

B. Background

6. The Uniform Rules constitute a new step in a series of international instruments adopted by UNCITRAL, which are either specifically focused on the needs of electronic commerce or were prepared bearing in mind the needs of modern means of communication. In the first category, specific instruments geared to electronic commerce comprise the Legal Guide on Electronic Funds Transfers (1987), the UNCITRAL Model Law on International Credit Transfers (1992) and the UNCITRAL Model Law on Electronic Commerce (1996 and 1998). The second category consists of all international conventions and other legislative instruments adopted by UNCITRAL since 1978, all of which promote reduced formalism and contain definitions of "writing" that are meant to encompass de-materialized communications.

7. The most specific (and possibly best known) UNCITRAL instrument in the field of electronic commerce is the UNCITRAL Model Law on Electronic Commerce. Its preparation in the early 1990s resulted from the increased use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions. It was realized that new technologies had been developing rapidly and would develop further as technical supports such as information highways and the Internet became more widely accessible. However, the communication of legally significant information in the form of paperless messages was hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. With a view to facilitating the increased use of modern means of communication, UNCITRAL has prepared the Model Law. The purpose of the Model Law is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce".

8. The decision by UNCITRAL to formulate model legislation on electronic

commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information was inadequate or outdated because it did not contemplate the use of electronic commerce. In certain cases, existing legislation still imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents. With respect to the notions of "written", "signed" and "original" documents, the Model Law adopted a functional-equivalent approach.

9. At the time when the Model Law was being prepared, a few countries had adopted specific provisions to deal with certain aspects of electronic commerce. However, there existed no legislation dealing with electronic commerce as a whole. This could result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Moreover, while sound laws and practices were necessary in all countries where the use of EDI and electronic mail was becoming widespread, this need was also felt in many countries with respect to such communication techniques as telecopy and telex.

10. The Model Law also helped to remedy disadvantages that stemmed from the fact that inadequate legislation at the national level created obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. To a large extent, disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may still contribute to limiting the extent to which businesses may access international markets.

11. Furthermore, at an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those States parties to such international instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

C. History

12. After adopting the UNCITRAL Model Law on Electronic Commerce, the Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [5]

13. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). The Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of legislation in that area. While no firm decision as to the form and content of such work had been reached, the Working Group had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of

electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157). The Commission endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities.

14. With respect to the exact scope and form of the Uniform Rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral approach taken in the Model Law. Thus, the Uniform Rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the Uniform Rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought. [6]

15. The Working Group began the preparation of the Uniform Rules at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73).

16. At its thirty-first session (1998), the Commission had before it the report of the Working Group on the work of its thirty-second session (A/CN.9/446). It was noted that the Working Group, throughout its thirty-first and thirty-second sessions, had experienced manifest difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital and other electronic signatures. It was also noted that a consensus was still to be found as to how those issues might be addressed in an internationally acceptable legal framework. However, it was generally felt by the Commission that the progress realized so far indicated that the draft Uniform Rules on Electronic Signatures were progressively being shaped into a workable structure.

17. The Commission reaffirmed the decision made at its thirtieth session as to the feasibility of preparing such Uniform Rules and expressed its confidence that more progress could be accomplished by the Working Group at its thirty-third session on the basis of the revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.76). In the context of that discussion, the Commission noted with satisfaction that the Working Group had become generally recognized as a particularly important international forum for the exchange of views regarding the legal issues of electronic commerce and for the preparation of solutions to those issues. [7]

18. The Working Group continued revision of the Uniform Rules at its thirty-third session (1998) and thirty-fourth session (1999) on the basis of notes prepared by the Secretariat (A/CN.9/WG.IV/WP.76 and A/CN.9/WG.IV/WP.79 and 80). The reports of the sessions are contained in documents A/CN.9/454 and 457.

19. At its thirty-second session (1999), the Commission had before it the report of the Working Group on the work of its thirty-third (June-July 1998) and thirty-fourth (February 1999) sessions (A/CN.9/454 and 457). The Commission expressed its appreciation for the efforts accomplished by the Working Group in its preparation of the

Uniform Rules. While it was generally agreed that significant progress had been made at those sessions in the understanding of the legal issues of electronic signatures, it was also felt that the Working Group had been faced with difficulties in the building of a consensus as to the legislative policy on which the uniform rules should be based.

20. A view was expressed that the approach currently taken by the Working Group did not sufficiently reflect the business need for flexibility in the use of electronic signatures and other authentication techniques. As currently envisaged by the Working Group, the Uniform Rules placed excessive emphasis on digital signature techniques and, within the sphere of digital signatures, on a specific application involving third-party certification. Accordingly, it was suggested that work on electronic signatures by the Working Group should either be limited to the legal issues of cross-border certification or be postponed altogether until market practices were better established. A related view expressed was that, for the purposes of international trade, most of the legal issues arising from the use of electronic signatures had already been solved in the UNCITRAL Model Law on Electronic Commerce. While regulation dealing with certain uses of electronic signatures might be needed outside the scope of commercial law, the Working Group should not become involved in any such regulatory activity.

21. The widely prevailing view was that the Working Group should pursue its task on the basis of its original mandate. With respect to the need for uniform rules on electronic signatures, it was explained that, in many countries, guidance from UNCITRAL was expected by governmental and legislative authorities that were in the process of preparing legislation on electronic signature issues, including the establishment of public-key infrastructures (PKI) or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by the Working Group to focus on PKI issues and PKI terminology, it was recalled that the interplay of relationships between three distinct types of parties (i.e., key holders, certification authorities and relying parties) corresponded to one possible PKI model, but that other models were conceivable, e.g., where no independent certification authority was involved. One of the main benefits to be drawn from focusing on PKI issues was to facilitate the structuring of the Uniform Rules by reference to three functions (or roles) with respect to key pairs, namely, the key issuer (or subscriber) function, the certification function, and the relying function. It was generally agreed that those three functions were common to all PKI models. It was also agreed that those three functions should be dealt with irrespective of whether they were in fact served by three separate entities or whether two of those functions were served by the same person (e.g., where the certification authority was also a relying party). In addition, it was widely felt that focusing on the functions typical of PKI and not on any specific model might make it easier to develop a fully media-neutral rule at a later stage (ibid., para. 68).

22. After discussion, the Commission reaffirmed its earlier decisions as to the feasibility of preparing such uniform rules and expressed its confidence that more progress could be accomplished by the Working Group at its forthcoming sessions. [8]

23. The Working Group continued its work at its thirty-fifth (September 1999) and thirty-sixth (February 2000) sessions on the basis of notes prepared by the Secretariat (A/CN.9/WG.IV/WP. 82 and 84). At its thirty-third (2000) session, the Commission had before it the report of the Working Group on the work of those two sessions (A/CN.9/465 and 467). It was noted that the Working Group, at its thirty-sixth session, had adopted the text of draft articles 1 and 3 to 12 of the Uniform Rules. It was stated that some issues remained to be clarified as a result of the decision by the Working Group to delete the notion of enhanced electronic signature from the draft Uniform Rules. A concern was expressed that, depending on the decisions to be made by the Working Group with respect to draft articles 2 and 13, the remainder of the draft provisions might need to be revisited to avoid creating a situation where the standard set

forth by the Uniform Rules would apply equally to electronic signatures that ensured a high level of security and to low-value certificates that might be used in the context of electronic communications that were not intended to carry significant legal effect.

24. After discussion, the Commission expressed its appreciation for the efforts extended by the Working Group and the progress achieved in the preparation of the draft Uniform Rules. The Working Group was urged to complete its work with respect to the draft Uniform Rules at its thirty-seventh session and to review the draft guide to enactment to be prepared by the Secretariat.[9] *[Note by the Secretariat: this section recording the history of the Uniform Rules is to be completed, and possibly made more concise, after final consideration and adoption of the Uniform Rules by the Commission].*

II. THE UNIFORM RULES AS A TOOL FOR HARMONIZING LAWS

25. As the Model Law, the Uniform Rules are in the form of a legislative text that is recommended to States for incorporation into their national law. Unlike an international convention, model legislation does not require the State enacting it to notify the United Nations or other States that may have also enacted it. However, States are strongly encouraged to inform the UNCITRAL Secretariat of any enactment of the Uniform Rules (or any other Model Law resulting from the work of UNCITRAL).

26. In incorporating the text of the model legislation into its legal system, a State may modify or leave out some of its provisions. In the case of a convention, the possibility of changes being made to the uniform text by the States parties (normally referred to as "reservations") is much more restricted; in particular trade law conventions usually either totally prohibit reservations or allow only very few, specified ones. The flexibility inherent in model legislation is particularly desirable in those cases where it is likely that the State would wish to make various modifications to the uniform text before it would be ready to enact it as national law. Some modifications may be expected in particular when the uniform text is closely related to the national court and procedural system. This, however, also means that the degree of, and certainty about, harmonization achieved through model legislation is likely to be lower than in the case of a convention. However, this relative disadvantage of model legislation may be balanced by the fact that the number of States enacting model legislation is likely to be higher than the number of States adhering to a convention. In order to achieve a satisfactory degree of harmonization and certainty, it is recommended that States make as few changes as possible in incorporating the Uniform Rules into their legal systems. In general, in enacting the Uniform Rules (or the Model Law), it is advisable to adhere as much as possible to the uniform text in order to make the national law as transparent as possible for foreign users of the national law.

III. GENERAL REMARKS ON ELECTRONIC SIGNATURES [10]

A. Functions of signatures

27. Article 7 of the UNCITRAL Model Law on Electronic Commerce is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the Model Law, the Working Group discussed the following functions traditionally performed by hand-written signatures: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature

could perform a variety of functions, depending on the nature of the document that was signed. For example, a signature might attest to: the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing); the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place. The relationship of the Uniform Rules with article 7 of the Model Law is further discussed below, in paragraphs 67 and 70 to 75 of this Guide.

28. In an electronic environment, the original of a message is indistinguishable from a copy, bears no handwritten signature, and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions. The purpose of various techniques currently available on the market or still under development is to offer the technical means by which some or all of the functions identified as characteristic of hand-written signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures".

B. Digital signatures and other electronic signatures

29. In discussing the desirability and feasibility of preparing the Uniform Rules, and in defining the scope of such Uniform Rules, UNCITRAL has examined various electronic signature techniques currently being used or still under development. The common purpose of those techniques is to provide functional equivalents to (1) hand-written signatures; and (2) other kinds of authentication mechanisms used in a paper-based environment (e.g., seals or stamps). The same techniques may perform additional functions in the sphere of electronic commerce, which are derived from the functions of a signature but correspond to no strict equivalent in a paper-based environment.

30. As indicated above, guidance from UNCITRAL is expected in many countries, by governmental and legislative authorities that are in the process of preparing legislation on electronic signature issues, including the establishment of public key infrastructures (PKI) or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by the UNCITRAL to focus on PKI issues and PKI terminology, it should be noted that the interplay of relationships between three distinct types of parties (i.e., signatories, suppliers of certification services and relying parties) corresponds to one possible PKI model, but other models are conceivable (e.g., where no independent certification authority is involved). One of the main benefits to be drawn from focusing on PKI issues is to facilitate the structuring of the Uniform Rules by reference to three functions (or roles) with respect to electronic signatures, namely, the signatory (key issuer or key subscriber) function, the certification function, and the relying function. Those three functions are common to all PKI models and should be dealt with irrespective of whether they are in fact served by three separate entities or whether two of those functions are served by the same person (e.g., where the supplier of certification services is also a relying party). Focusing on the functions performed in a PKI environment and not on any specific model also makes it easier to develop a fully media-neutral rule to the extent that similar functions are served in non-PKI electronic signature technology.

1. Electronic signatures relying on techniques other than public-key cryptography

31. Alongside "digital signatures" based on public-key cryptography, there exist various other devices, also covered in the broader notion of "electronic signature" mechanisms, which may currently be used, or considered for future use, with a view to fulfilling one or more of the above-mentioned functions of handwritten signatures. For example, certain techniques would rely on authentication through a biometrical device

based on hand-written signatures. In such a device, the signatory would sign manually, using a special pen, either on a computer screen or on a digital pad. The hand-written signature would then be analysed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the recipient for authentication purposes. Such an authentication system would presuppose that samples of the handwritten signature have been previously analysed and stored by the biometrical device.

32. Little information was provided to the UNCITRAL Working Group on Electronic Commerce in the preparation of the Uniform Rules as to the technical and legal implications of using "signature" devices relying on techniques other than public-key cryptography. In view of the availability of sufficient preliminary information as to the legal implications of digital signatures, and of the existence of draft legislation on the topic in a number of countries, the work of UNCITRAL focused on issues of digital signatures relying on public-key cryptography.

33. However, UNCITRAL has intended to develop Uniform Rules that can facilitate the use of both digital signatures and other forms of electronic signatures. To that effect, UNCITRAL has attempted to deal with the legal issues of electronic signature issues at a level that is intermediate between the high generality of the Model Law and the specificity that might be required when dealing with a given signature technique. In any event, consistent with media neutrality in the Model Law, the Uniform Rules are not to be interpreted as discouraging the use of any method of electronic signature, whether already existing or to be implemented in the future.

2. *Digital signatures relying on public-key cryptography* [11]

34. In view of the increasing use of digital signature techniques in a number of countries, the following introduction may be of assistance to those preparing legislation on electronic signatures.

(a) Technical notions and terminology

(i) Cryptography

35. Digital signatures are created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form. Digital signatures use what is known as "public key cryptography", which is often based on the use of algorithmic functions to generate two different but mathematically-related "keys" (i.e., large numbers produced using a series of mathematical formulae applied to prime numbers). One such key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other one for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms.

36. While the use of cryptography is one of the main features of digital signatures, the mere fact that a digital signature is used to authenticate a message containing information in digital form should not be confused with a more general use of cryptography for confidentiality purposes. Confidentiality encryption is a method used for encoding an electronic communication so that only the originator and the addressee of the message will be able to read it. In a number of countries, the use of cryptography for confidentiality purposes is limited by law for reasons of public policy that may involve considerations of national defence. However, the use of cryptography for

authentication purposes by producing a digital signature does not necessarily imply the use of encryption to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message.

(ii) Public and private keys

37. The complementary keys used for digital signatures are named the "private key", which is used only by the signatory to create the digital signature, and the "public key", which is ordinarily more widely known and is used by a relying party to verify the digital signature. The user of a private key is expected to keep the private key secret. It should be noted that the individual user does not need to know the private key. Such a private key is likely to be kept on a smart card, or to be accessible through a personal identification number or, ideally, through a biometrical identification device, e.g., through thumbprint recognition. If many people need to verify the signatory's digital signatures, the public key must be available or distributed to all of them, for example by publication in an on-line repository or any other form of public directory where it is easily accessible. Although the keys of the pair are mathematically related, if an asymmetric cryptosystem has been designed and implemented securely it is virtually infeasible to derive the private key from knowledge of the public key. The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is particularly difficult and time-consuming to determine which two prime numbers created that new, larger number. [12] Thus, although many people may know the public key of a given signatory and use it to verify that signatory's signatures, they cannot discover that signatory's private key and use it to forge digital signatures.

38. It should be noted, however, that the concept of public-key cryptography does not necessarily imply the use of the above-mentioned algorithms based on prime numbers. Other mathematical techniques are currently used or under development, such as cryptosystems relying on elliptic curves, which are often described as offering a high degree of security through the use of significantly reduced key-lengths.

(iii) Hash function

39. In addition to the generation of key pairs, another fundamental process, generally referred to as a "hash function", is used in both creating and verifying a digital signature. A hash function is a mathematical process, based on an algorithm which creates a digital representation, or compressed form of the message, often referred to as a "message digest", or "fingerprint" of the message, in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes named a "one-way hash function", it is virtually impossible to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

(iv) Digital signature

40. To sign a document or any other item of information, the signatory first delimits precisely the borders of what is to be signed. Then a hash function in the signatory's software computes a hash result unique (for all practical purposes) to the information to

be signed. The signatory's software then transforms the hash result into a digital signature using the signatory's private key. The resulting digital signature is thus unique to both the information being signed and the private key used to create the digital signature.

41. Typically, a digital signature (a digitally signed hash result of the message) is attached to the message and stored or transmitted with that message. However, it may also be sent or stored as a separate data element, as long as it maintains a reliable association with the corresponding message. Since a digital signature is unique to its message, it is useless if permanently disassociated from the message.

(v) Verification of digital signature

42. Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key, and whether the newly computed hash result matches the original hash result that was transformed into the digital signature during the signing process.

43. The verification software will confirm the digital signature as "verified" if: (1) the signatory's private key was used to sign digitally the message, which is known to be the case if the signatory's public key was used to verify the signature because the signatory's public key will verify only a digital signature created with the signatory's private key; and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

(b) Public key infrastructure (PKI) and suppliers of certification services

44. To verify a digital signature, the verifier must have access to the signatory's public key and have assurance that it corresponds to the signatory's private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. If public key encryption is to serve its intended purposes, it needs to provide a way to send keys to a wide variety of persons, many of whom are not known to the sender, where no relationship of trust has developed between the parties. To that effect, the parties involved must have a high degree of confidence in the public and private keys being issued.

45. The requested level of confidence may exist between parties who trust each other, who have dealt with each other over a period of time, who communicate on closed systems, who operate within a closed group, or who are able to govern their dealings contractually, for example, in a trading partner agreement. In a transaction involving only two parties, each party can simply communicate (by a relatively secure channel such as a courier or telephone, with its inherent feature of voice recognition) the public key of the key pair each party will use. However, the same level of confidence may not be present when the parties deal infrequently with each other, communicate over open systems (e.g., the World Wide Web on the Internet), are not in a closed group, or do not have trading partner agreements or other law governing their relationships.

46. In addition, because public key encryption is a highly mathematical technology, all users must have confidence in the skill, knowledge and security arrangements of the parties issuing the public and private keys. [13]

47. A prospective signatory might issue a public statement indicating that signatures verifiable by a given public key should be treated as originating from that signatory. However, other parties might be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of inadvertently trusting an imposter, or of having to disprove a false denial of a digital signature (an issue often referred to as "non-repudiation") if a transaction should turn out to prove disadvantageous for the purported signatory.

48. A solution to these problems is the use of one or more trusted third parties to associate an identified signatory or the signatory's name with a specific public key. That trusted third party is generally referred to as a "certification authority", "certification services provider" or "supplier of certification services" in most technical standards and guidelines (in the Uniform Rules, the term "supplier of certification services" has been chosen). In a number of countries, such certification authorities are being organized hierarchically into what is often referred to as a public key infrastructure (PKI).

(i) Public key infrastructure (PKI)

49. Setting up a public key infrastructure (PKI) is a way to provide confidence that: (1) a user's public key has not been tampered with and in fact corresponds to that user's private key; (2) the encryption techniques being used are sound; (3) the entities that issue the cryptographic keys can be trusted to retain or recreate the public and private keys that may be used for confidentiality encryption where the use of such a technique is authorized; (4) different encryption systems are inter-operable. To provide the confidence described above, a PKI may offer a number of services, including the following: (1) managing cryptographic keys used for digital signatures; (2) certifying that a public key corresponds to a private key; (3) providing keys to end users; (4) deciding which users will have which privileges on the system; (5) publishing a secure directory of public keys or certificates; (6) managing personal tokens (e.g., smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (7) checking the identification of end users, and providing them with services; (8) providing non-repudiation services; (9) providing time-stamping services; (10) managing encryption keys used for confidentiality encryption where the use of such a technique is authorized.

50. A public key infrastructure (PKI) is often based on various hierarchical levels of authority. For example, models considered in certain countries for the establishment of possible PKIs include references to the following levels: (1) a unique "root authority", which would certify the technology and practices of all parties authorized to issue cryptographic key pairs or certificates in connection with the use of such key pairs, and would register subordinate certification authorities;[14] (2) various certification authorities, placed below the "root" authority, which would certify that a user's public key actually corresponds to that user's private key (i.e., has not been tampered with); and (3) various local registration authorities, placed below the certification authorities, and receiving requests from users for cryptographic key pairs or for certificates in connection with the use of such key pairs, requiring proof of identification and checking identities of potential users. In certain countries, it is envisaged that notaries public might act as, or support, local registration authorities.

51. The issues of PKI may not lend themselves easily to international harmonization. The organization of a PKI may involve various technical issues, as well as issues of public policy that may better be left to each individual State at the current stage.[15] In that connection, decisions may need to be made by each State considering the establishment of a PKI, for example as to: (1) the form and number of levels of authority which should be comprised in a PKI; (2) whether only certain authorities belonging to the PKI should be allowed to issue cryptographic key pairs or whether such key pairs might be issued by the users themselves; (3) whether the certification authorities certifying the validity of cryptographic key pairs should be public entities or whether private entities might act as certification authorities; (4) whether the process of allowing a given entity to act as a certification authority should take the form of an express authorization, or "licensing", by the State, or whether other methods should be used to control the quality of certification authorities if they were allowed to operate in the absence of a specific authorization; (5) the extent to which the use of cryptography should be authorized for confidentiality purposes; and (6) whether Government authorities should retain access to encrypted information, through a mechanism of "key escrow" or otherwise. The Uniform Rules do not deal with those issues.

(ii) Supplier of certification services

52. To associate a key pair with a prospective signatory, a supplier of certification services (or certification authority) issues a certificate, an electronic record which lists a public key together with the name of the certificate subscriber as the "subject" of the certificate, and may confirm that the prospective signatory identified in the certificate holds the corresponding private key. The principal function of a certificate is to bind a public key with a particular holder. A "recipient" of the certificate desiring to rely upon a digital signature created by the holder named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, assurance is provided that the digital signature was created by the holder of the public key named in the certificate, and that the corresponding message had not been modified since it was digitally signed.

53. To assure the authenticity of the certificate with respect to both its contents and its source, the certification authority digitally signs it. The issuing certification authority's digital signature on the certificate can be verified by using the public key of the certification authority listed in another certificate by another certification authority (which may but need not be on a higher level in a hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. In each case, the issuing certification authority must digitally sign its own certificate during the operational period of the other certificate used to verify the certification authority's digital signature.

54. A digital signature corresponding to a message, whether created by the holder of a key pair to authenticate a message or by a certification authority to authenticate its certificate, should generally be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the "operational period" stated in the certificate, which is a condition of the verifiability of a digital signature.

55. To make a public key and its correspondence to a specific holder readily available for verification, the certificate may be published in a repository or made available by other means. Typically, repositories are on-line databases of certificates and other information available for retrieval and use in verifying digital signatures.

56. Once issued, a certificate may prove to be unreliable, for example in situations

where the holder misrepresents its identity to the certification authority. In other circumstances, a certificate may be reliable enough when issued but it may become unreliable sometime thereafter. If the private key is "compromised", for example through loss of control of the private key by its holder, the certificate may lose its trustworthiness or become unreliable, and the certification authority (at the holder's request or even without the holder's consent, depending on the circumstances) may suspend (temporarily interrupt the operational period) or revoke (permanently invalidate) the certificate. Immediately upon suspending or revoking a certificate, the certification authority is generally expected to publish notice of the revocation or suspension or notify persons who enquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

57. Certification authorities could be operated by Government authorities or by private sector service providers. In a number of countries, it is envisaged that, for public policy reasons, only Government entities should be authorized to operate as certification authorities. In other countries, it is considered that certification services should be open to competition from the private sector. Irrespective of whether certification authorities are operated by public entities or by private sector service providers, and of whether certification authorities would need to obtain a license to operate, there is typically more than one certification authority operating within the PKI. Of particular concern is the relationship between the various certification authorities. Certification authorities within a PKI can be established in a hierarchical structure, where some certification authorities only certify other certification authorities, which provide services directly to users. In such a structure, certification authorities are subordinate to other certification authorities. In other conceivable structures, some certification authorities may operate on an equal footing with other certification authorities. In any large PKI, there would likely be both subordinate and superior certification authorities. In any event, in the absence of an international PKI, a number of concerns may arise with respect to the recognition of certificates by certification authorities in foreign countries. The recognition of foreign certificates is often achieved by a method called "cross certification". In such a case, it is necessary that substantially equivalent certification authorities (or certification authorities willing to assume certain risks with regard to the certificates issued by other certification authorities) recognize the services provided by each other, so their respective users can communicate with each other more efficiently and with greater confidence in the trustworthiness of the certificates being issued.

58. Legal issues may arise with regard to cross-certifying or chaining of certificates when there are multiple security policies involved. Examples of such issues may include determining whose misconduct caused a loss, and upon whose representations the user relied. It should be noted that legal rules considered for adoption in certain countries provide that, where the levels of security and policies are made known to the users, and there is no negligence on the part of certification authorities, there should be no liability.

59. It may be incumbent upon the certification authority or the root authority to ensure that its policy requirements are met on an ongoing basis. While the selection of certification authorities may be based on a number of factors, including the strength of the public key being used and the identity of the user, the trustworthiness of any certification authority may also depend on its enforcement of certificate-issuing standards and the reliability of its evaluation of data received from users who request certificates. Of particular importance is the liability regime applying to any certification authority with respect to its compliance with the policy and security requirements of the root authority or superior certification authority, or with any other applicable requirement, on an ongoing basis.

60. In the preparation of the Uniform Rules, the following elements were considered as possible factors to be taken into account when assessing the trustworthiness of a certification authority: (1) independence (i.e., absence of financial or other interest in underlying transactions); (2) financial resources and financial ability to bear the risk of being held liable for loss; (3) expertise in public-key technology and familiarity with proper security procedures; (4) longevity (certification authorities may be required to produce evidence of certification or decryption keys many years after the underlying transaction has been completed, in the context of a lawsuit or property claim); (5) approval of hardware and software; (6) maintenance of an audit trail and audit by an independent entity; (7) existence of a contingency plan (e.g., "disaster recovery" software or key escrow); (8) personnel selection and management; (9) protection arrangements for the certification authority's own private key; (10) internal security; (11) arrangements for termination of operations, including notice to users; (12) warranties and representations (given or excluded); (13) limitation of liability; (14) insurance; (15) inter-operability with other certification authorities; (16) revocation procedures (in cases where cryptographic keys might be lost or compromised).

(c) Summary of the digital signature process

61. The use of digital signatures usually involves the following processes, performed either by the signatory or by the receiver of the digitally signed message:

(1) The user generates or is given a unique cryptographic key pair;

(2) The sender prepares a message (for example, in the form of an electronic mail message) on a computer;

(3) The sender prepares a "message digest", using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key;

(4) The sender encrypts the message digest with the private key. The private key is applied to the message digest text using a mathematical algorithm. The digital signature consists of the encrypted message digest;

(5) The sender typically attaches or appends its digital signature to the message;

(6) The sender sends the digital signature and the (unencrypted or encrypted) message to the recipient electronically;

(7) The recipient uses the sender's public key to verify the sender's digital signature. Verification using the sender's public key proves that the message came exclusively from the sender;

(8) The recipient also creates a "message digest" of the message, using the same secure hash algorithm;

(9) The recipient compares the two message digests. If they are the same, then the recipient knows that the message has not been altered after it was signed. Even if one bit in the message has been altered after the message has been digitally signed, the message digest created by the recipient will be different from the message digest created by the sender;

(10) The recipient obtains a certificate from the certification authority (or via the originator of the message), which confirms the digital signature on the sender's message. The certification authority is typically a trusted third party which administers certification in the digital signature system. The certificate contains the public key and name of the sender (and possibly additional information), digitally signed by the certification authority.

IV. MAIN FEATURES OF THE UNIFORM RULES

A. Legislative nature of the Uniform Rules

62. The Uniform Rules were prepared on the assumption that they should be directly derived from article 7 of the Model Law and should be considered as a way to provide detailed information as to the concept of a reliable "method used to identify" a person and "to indicate that person's approval" of the information contained in a data message (see A/CN.9/WG.IV/WP.71, para. 49).

63. The question of what form the draft Uniform Rules might take was raised and the importance of considering the relationship of the form to the content was noted. Different approaches were suggested as to what the form might be, which included contractual rules, legislative provisions, or guidelines for States considering enacting legislation on electronic signatures. It was agreed as a working assumption that the Uniform Rules should be prepared as legislative rules with commentary, and not merely as guidelines (see A/CN.9/437, para. 27; A/CN.9/446, para. 25; and A/CN.9/457, paras. 51 and 72).

B. Relationship with the UNCITRAL Model Law on Electronic Commerce

1. Uniform Rules as a separate legal instrument

64. The Uniform Rules could have been incorporated in an extended version of the Model Law, for example to form a new part III of the Model Law. With a view to indicating clearly that the Uniform Rules could be enacted either independently or in combination with the Model Law, it was eventually decided that the Uniform Rules should be prepared as a separate legal instrument (see A/CN.9/465, para. 37). That decision results mainly from the fact that, at the time the Uniform Rules were being finalized, the Model Law had already been successfully implemented in a number of countries and was being considered for adoption in many other countries. The preparation of an extended version of the Model Law might have compromised the success of the original version by suggesting a need to improve on that text by way of an update. In addition, preparing a new version of the Model Law might have introduced confusion in those countries that had recently adopted the Model Law.

2. Uniform Rules fully consistent with the Model Law

65. In drafting the Uniform Rules, every effort was made to ensure consistency with both the substance and the terminology of the Model Law (A/CN.9/465, para. 37). The general provisions of the Model Law have been reproduced in the Uniform Rules. These are articles 1 (Sphere of application), 2(a),(c) and (e) (Definitions of "data message", "originator" and "addressee"), 3 (Interpretation), 4 (Variation by agreement) and 7 (Signature) of the Model Law.

66. Based on the Model Law, the Uniform Rules are intended to reflect in particular: the principle of media-neutrality; an approach under which functional equivalents of

traditional paper-based concepts and practices should not be discriminated against; and extensive reliance on party autonomy (A/CN.9/WG.IV/WP.84, para. 16). They are intended for use both as minimum standards in an "open" environment (i.e., where parties communicate electronically without prior agreement) and as default rules in a "closed" environment (i.e., where parties are bound by pre-existing contractual rules and procedures to be followed in communicating by electronic means).

3. Relationship with article 7 of the Model Law

67. In the preparation of the Uniform Rules, the view was expressed that the reference to article 7 of the Model Law in the text of article 6 of the Uniform Rules was to be interpreted as limiting the scope of the Uniform Rules to situations where an electronic signature was used to meet a mandatory requirement of law that certain documents had to be signed for *validity* purposes. Under that view, since the law contained very few such requirements with respect to documents used for commercial transactions, the scope of the Uniform Rules was very narrow. It was generally agreed, in response, that such interpretation of draft article 6 (and of article 7 of the Model Law) was inconsistent with the interpretation of the words "the law" adopted by the Commission in paragraph 68 of the Guide to Enactment of the Model Law, under which "the words 'the law' are to be understood as encompassing not only statutory or regulatory law but also judicially-created law and other procedural law". In fact, the scope of both article 7 of the Model Law and article 6 of the Uniform Rules is particularly broad, since most documents used in the context of commercial transactions are likely to be faced, in practice, with the requirements of the law of evidence regarding proof in writing (A/CN.9/465, para. 67).

C. "Framework" rules to be supplemented by technical regulations and contract

68. As a supplement to the UNCITRAL Model Law on Electronic Commerce, the Uniform Rules are intended to provide essential principles for facilitating the use of electronic signatures. However, as a "framework", the Uniform Rules themselves do not set forth all the rules and regulations that may be necessary (in addition to contractual arrangements between users) to implement those techniques in an enacting State. Moreover, as indicated in this Guide, the Uniform Rules are not intended to cover every aspect of the use of electronic signatures. Accordingly, an enacting State may wish to issue regulations to fill in the procedural details for procedures authorized by the Uniform Rules and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Uniform Rules. It is recommended that, should it decide to issue such regulation, an enacting State should give particular attention to the need to preserve flexibility in the operation of electronic signature systems by their users.

69. It should be noted that the electronic signature techniques considered in the Uniform Rules, beyond raising matters of procedure that may need to be addressed in the implementing technical regulations, may raise certain legal questions, the answers to which will not necessarily be found in the Uniform Rules, but rather in other bodies of law. Such other bodies of law may include, for example, the applicable administrative, contract, criminal and judicial-procedure law, which the Uniform Rules are not intended to deal with.

D. Added certainty as to the legal effects of electronic signatures

70. One of the main features of the Uniform Rules is to add certainty to the operation of the flexible criterion set forth in article 7 of the Model Law for the recognition of an electronic signature as functionally equivalent to a hand-written signature.

Article 7 of the Model Law reads as follows:

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

"(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

"(3) The provisions of this article do not apply to the following: [...]".

71. Article 7 is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the Model Law, the following functions of a signature were considered: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text; the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place.

72. With a view to ensuring that a message that was required to be authenticated should not be denied legal value for the sole reason that it was not authenticated in a manner peculiar to paper documents, article 7 adopts a comprehensive approach. It establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements that currently present barriers to electronic commerce. Article 7 focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document. Paragraph (1)(a) establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.

73. Paragraph (1)(b) establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph (1)(a). The method used under paragraph (1)(a) should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all the circumstances, including any agreement between the originator and the addressee of the data message.

74. In determining whether the method used under paragraph (1) is appropriate, legal, technical and commercial factors that may be taken into account include the following: (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by

any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, paras. 53 and 56 to 58).

75. Building on the flexible criterion expressed in article 7(1)(b) of the Model Law, articles 6 and 7 of the Uniform Rules establish a mechanism through which electronic signatures that meet objective criteria of technical reliability can be made to benefit from early determination as to their legal effectiveness. The effect of the Uniform Rules is to recognize two categories of electronic signatures. The first and broader category is that described in article 7 of the Model Law. It consists of any "method" that may be used to fulfil a legal requirement for a hand-written signature. The legal effectiveness of such a "method" as an equivalent of a hand-written signature depends upon demonstration of its "reliability" to a trier of fact. The second and narrower category is that created by the Uniform Rules. It consists of methods of electronic signature that may be recognized by a State authority, a private accredited entity, or the parties themselves, as meeting the criteria of technical reliability set forth in the Uniform Rules. The advantage of such a recognition is that it brings certainty to the users of such electronic signature techniques (sometimes referred to as "enhanced", "secure" or "qualified" electronic signatures) before they actually use the electronic signature technique.

E. Basic rules of conduct for the parties involved

76. The Uniform Rules do not deal in any detail with the issues of liability that may affect the various parties involved in the operation of electronic signature systems. Those issues are left to applicable law outside the Uniform Rules. However, the Uniform Rules set out criteria against which to assess the conduct of those parties, i.e., the signatory, the relying party and the supplier of certification services.

77. As to the signatory, the Uniform Rules elaborate on the basic principle that the signatory should apply reasonable care with respect to its electronic signature device. The signatory is expected to exercise reasonable care to avoid unauthorized use of that signature device. Where the signatory knows or should have known that the signature device has been compromised, the signatory should give notice without undue delay to any person who may reasonably be expected to rely on, or to provide services in support of, the electronic signature. Where a certificate is used to support the electronic signature, the signatory is expected to exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory in connection with the certificate.

78. A relying party is expected to take reasonable steps to verify the reliability of an electronic signature. Where the electronic signature is supported by a certificate, the relying party should take reasonable steps to verify the validity, suspension or revocation of the certificate, and observe any limitation with respect to the certificate.

79. The general duty of a supplier of certification services is to utilize trustworthy systems, procedures and human resources, and to act in accordance with representations that the supplier makes with respect to its policies and practices. In addition, the supplier of certification services is expected to exercise reasonable care to ensure the accuracy and completeness of all material representations it makes in connection with a certificate. In the certificate, the supplier should provide essential information allowing

the relying party to identify the supplier. It should also represent that: (1) the person who is identified in the certificate had control of the signature device at the time of signing; and (2) the signature device was operational on or before the date when the certificate was issued. In its dealings with the relying party, the supplier of certification services should provide additional information as to: (1) the method used to identify the signatory; (2) any limitation on the purpose or value for which the signature device or the certificate may be used; (3) the operational condition of the signature device; (4) any limitation on the scope or extent of liability of the supplier of certification services; (5) whether means exist for the signatory to give notice that a signature device has been compromised; and (6) whether a timely revocation service is offered.

80. For the assessment of the trustworthiness of the systems, procedures and human resources utilized by the supplier of certification services, the Uniform Rules provide an open-ended list of indicative factors.

F. A technology-neutral framework

81. Given the pace of technological innovation, the Uniform Rules provide for the legal recognition of electronic signatures irrespective of the technology used (e.g., digital signatures relying on asymmetric cryptography, or biometrics).

V. ASSISTANCE FROM THE UNCITRAL SECRETARIAT

A. Assistance in drafting legislation

82. In the context of its training and assistance activities, the UNCITRAL secretariat assists States with technical consultations for the preparation of legislation based on the UNCITRAL Uniform Rules on Electronic Signatures. The same assistance is brought to Governments considering legislation based on other UNCITRAL model laws, or considering adhesion to one of the international trade law conventions prepared by UNCITRAL.

83. Further information concerning the Uniform Rules and other model laws and conventions developed by UNCITRAL, may be obtained from the secretariat at the address below:

International Trade Law Branch, Office of Legal Affairs
United Nations
Vienna International Centre
P.O. Box 500
A-1400, Vienna, Austria

Telephone:	(+43-1) 26060-4060 or 4061
Telecopy:	(+43-1) 26060-5813
Electronic mail:	uncitral@uncitral.org
Internet Home Page:	http://www.uncitral.org

B. Information on the interpretation of legislation based on the Uniform Rules

84. The secretariat welcomes comments concerning the Uniform Rules and the Guide, as well as information concerning enactment of legislation based on the Uniform Rules. Once enacted, the Uniform Rules will be included in the CLOUT information system, which is used for collecting and disseminating information on case law relating to the conventions and model laws that have emanated from the work of UNCITRAL.

The purpose of the system is to promote international awareness of the legislative texts formulated by UNCITRAL and to facilitate their uniform interpretation and application. The secretariat publishes, in the six official languages of the United Nations, abstracts of decisions and makes available, against reimbursement of copying expenses, the decisions on the basis of which the abstracts were prepared. The system is explained in a user's guide that is available from the secretariat in hard copy (A/CN.9/SER.C/GUIDE/1) and on the above-mentioned Internet home page of UNCITRAL.

Notes

[1] *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), paras. 223-224.

[2] Ibid., *Fifty-second Session, Supplement No. 17* (A/52/17), paras. 249-251.

[3] A/CN.9/467, paras. 18-20.

[4] Official Records of the General Assembly, Fifty-fifth Session, Supplement No. 17 (A/55/17), paras. 380-383.

[5] *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), paras. 223-224.

[6] Ibid., *Fifty-second Session, Supplement No. 17* (A/52/17), paras. 249-251.

[7] Ibid., *Fifty-third Session, Supplement No. 17* (A/53/17), paras. 207-211.

[8] Ibid., *Fifty-fourth Session, Supplement No. 17* (A/54/17), paras. 308-314.

[9] Ibid., *Fifty-fifth Session, Supplement No. 17* (A/55/17), paras. 380-383.

[10] This section is drawn from document A/CN.9/WG.IV/WP.71, part I.

[11] Numerous elements of the description of the functioning of a digital signature system in this section are based on the ABA Digital Signature Guidelines, p. 8 to 17.

[12] Certain existing standards such as the ABA Digital Signature Guidelines refer to the notion of "computational infeasibility" to describe the expected irreversibility of the process, i.e., the hope that it will be impossible to derive a user's secret private key from that user's public key. "Computationally infeasible" is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance" (ABA Digital Signature Guidelines, p. 9, note 23).

[13] In situations where public and private cryptographic keys would be issued by the users themselves, such confidence might need to be provided by the certifiers of public keys.

[14] The question as to whether a government should have the technical ability to retain or recreate private confidentiality keys may be dealt with at the level of the root authority.

[15] However, in the context of cross-certification, the need for global interoperability requires that PKIs established in various countries should be capable of communicating with each other.